The Thesis Committee for Aditya Tyagi
Certifies that this is the approved version of the following Thesis:

Early Warning Identity Threat and Mitigation System

APPROVED BY
SUPERVISING COMMITTEE:

Suzanne Barber, Supervisor

Razieh Nokhbeh Zaeem

Early Warning Identity Threat and Mitigation System

by

Aditya Tyagi

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

May 2021

Dedication

First and foremost, I would like to thank God for helping believe in myself in seeing this work through. Through all the ups and downs in my life, I have never felt alone. May he bless everyone as he has blessed me.

I dedicate this work to my parents and sister. Their kind words of encouragement and evergreen support is what molded my academic interest in research and the needed resilience to dedicate my time in research projects. Through any hurdle I faced, ready to give up, they always stood by me ready to support me in any way they can. My family's love and support are one of the biggest motivators to help me see this project through.

I dedicate this work to my girlfriend and friends. From the late-night study sessions, last-minute cancelled plans, to the constant checking up on me through the duration of the project, they have been helping me with anything I need. Their understanding nature and on-the-fly solutions for any new problem helped me prioritize my work.

I dedicate this work to everyone around me who has showered me with nothing but love and support for encouraging me to complete the work.

Acknowledgements

I would like to acknowledge Dr. Suzanne Barber – professor and head of UT Austin Center for Identity – for her continued support throughout the project. Her class in Information, Security, and Privacy inspired me to choose the track as my academic and industry career. The opportunities she provided me with, be it teaching assistance or research assistance, helped me learn a lot in the field. Her constant support and mentorship have been one of the key factors to see this research through. I am extremely grateful to have her as my professor and as my supervisor. It has been a great honor to study and research under her guidance.

I would also like to express my sincere gratitude towards Dr. Razieh Nokhbeh Zaeem. Her consistent supervision throughout my thesis has helped me work on the project. Be it any question or request, Razieh has always helped me see through the issue. From administration issue to help in research, her guidance has helped me learn more about the topic and create this thesis. As a research supervisor, Razieh excels in motivating her subordinates and helping them deliver the best results they can. She has worked with me through all my hurdles in research and writing with extreme patience and mentorship. I whole-heartedly thank her for believing in me, this research, and helping me deliver the best results that I could.

I would also like to acknowledge The Center of Identity for letting me access the databases created for ITAP. The creation of the manually parsed database gave me the needed information for creation of my work. I acknowledge all the researchers' hard work in creating the ITAP dataset.

Abstract

Early Warning Identity Threat and Mitigation System

Aditya Tyagi, MSE

The University of Texas at Austin, 2021

Supervisor: Suzanne Barber

While many organizations share threat intelligence, there is still a lack of actionable data for organizations to proactively and effectively respond to emerging identity threats to mitigate a wide range of crimes. There currently exists no solution for organizations to access current trends and intelligence to understand emerging threats and how to appropriately respond to them. This research project delivers I-WARN, to help bridge that gap. Using a wide range of open-source information, I-WARN gathers, analyzes, and reports on threats related to the theft, fraud, and abuse of Personal Identifiable Information (PII). Then maps those threats to the MITRE ATT&CK framework to offer mitigation and risk reduction tactics. I-WARN aims to deliver actionable intelligence, offering early warning into threat behaviors, and mitigation responses. This thesis discusses the technical details of I-WARN, current solutions for threat intelligence sharing with how they compare to I-WARN, and future work.

Table of Contents

List of Tables ix

List of Figures x

Chapter 1: Introduction 1

Threat Intelligence: Concept 2

Information Sharing and its Facilitation 4

Opportunities from Information Sharing Facilitation 7

Chapter 2: Related Work 9

Information Sharing Outside of the United States 9

Within US: Fedeal Law Enforcement 10

Within US: CISA Alerts 12

Within US: Academic Work in Information Sharing 14

Within US: Non-Academic Work in Information Sharing 15

Threat Intelligence Companies 17

Chapter 3: System Overview 20

System Overview 20

ITAP Dataset 21

Mapping Threats to I-WARN 23

Organize Market Sector 25

Combining Extracted Information 28

Additional Features 28

GUI 29

Chapter 4: System Testing 34
Formal Systems 36
Informal Systems 40
Chapter 5: Future Work 44
Keeping the Sytem Open-Source and Live 44
Collecting Information from more Sources 44
Using Machine Leaerning 45
Incorporating all MITRE Techniques 46
Chapter 6: Conclusion 48
Bibliography 50

List of Tables

Table 1: Tables show a list of features for Virustotal and IBM X Force, respectively. It compares the features offered as part of their free services versus what the customer misses out by not opting in paid subscriptions [33]. Table 1 is not an exhaustive list of the features available on each platform. 18

Table 2: A snippet of the ITAP dataset with inputs, outputs, and steps taken by the bad actor. It also depicts the loss incurred by victims as well as countermeasures deployed. Aspects of counter measure with PII have been redacted. Information contained in the table for each story is not exhaustive. 22

Table 3: Table shows all the keywords from ITAP dataset used to create the scoring system. All inputs were grouped prior to mapping them to the threat tactics. More information about the overlaps can be found here: Link to Logic Map. 27

Table 4: Different systems and how they compare with I-WARN. 35

List of Figures

Figure 1: A Snippet from the MITRE ATT&CK framework where cyber incidents are linked to more detail and their lateral incident response tactics [10].....7

Figure 2: A snippet from the CISA Alert AA20-258A showing MITRE ATT&CK implementation, facilitating easier diffusion of information between CISA and the public [26]. 13

Figure 3: High-level overview of the system where the lifecycle of each story – from ITAP dataset to the frontend – is shown. 21

Figure 4: A snippet from the code showing the dictionary that is used to eliminate unnecessary techniques which are not seen in the ITAP dataset due to the high technical knowledge required. 26

Figure 5: Snippet from the GUI. The first one shows the webpage, as well as the pie chart showing the number of cases in each market sector. The education trends for threat tactics can also be seen, based off the current ITAP dataset.....31

Figure 6: The image shows the granularity of each story, divided by each sector. Each story has the description for top threat tactics used as well as hyperlinked mitigation suggestions, followed by the priority mitigation suggestion. 32

Figure 7: Image shows the CISA alert tab that also shows how much information each alert carries, and how the technical details can be mapped with MITRE ATT&CK matrix. 33

Figure 8: Snippet from an alert posted by the ACSC [36] that shows the main components of these alerts: background, mitigation tactics, and additional information. It is also interesting to see a reference to CISA as part of their mitigation response to understand more about the given IOCs. We compare the alert to I-WARN and conclude that the content and style of delivery is similar. 38

Figure 9: A small snippet of the alerts posted by CIS. The alerts give an overview of the advisory, currently affected systems as per the CVE, and mitigation responses. The content of each alert is like I-WARN since they focus on brief mitigation tactics and links for further, in-depth dive on each response. CIS, just like I-WARN, utilizes standard visualization and content delivery as federal and state agencies in the US. 39

Figure 10: A tweet snapshotted from The Hacker News showing us information sharing through Twitter – part of OSINT. Although the information is informal and lacks all the contents of detection and mitigation tactics, as seen in CISA and I-WARN, the time of delivery is significantly lower due to its informal style of delivery. 41

Figure 10: Snippet of the website Cyware and its alerts and notifications for cyber incidents that are not related to policies. It should be noted that Cyware does not create these articles and only curates them. This results in Cyware linking other websites like The Hacker News that may not have all the information for a proactive or reactive response. 42

Chapter 1: *Introduction*

This research offers early warning of identity threats along with proactive mitigation and response tactics to better equip organizations with the situation awareness and response tools necessary to thwart and combat identity crimes.

This chapter overviews significant advances in threat intelligence as offered by this research and captured in the delivered I-WARN system. I-WARN offers timely threat information sharing and delivers timely actionable intelligence for decision-makers by leveraging a wealth of information and expertise found in the University of Texas Center for Identity's (UT CID) Identity Threat Assessment and Prediction (ITAP) [13], the MITRE ATT&CK framework and a wide range of open sources.

With the world getting smaller through growing cyberspace, being connected with someone on the other side of the globe has never been easier. Unfortunately, that connectedness is used as an exploit. Digital footprints are becoming more exposed to the public; individuals and organizations are encouraged to understand the risk of exposure their identity-related tokens hold.

This research focuses on attacks relating with Personally Identifiable Information (PII): attributes of personal data vulnerable to reveal sensitive information about an individual. We also focus on other sensitive information such as financial records, healthcare records, and affiliated business records. When discussing intelligence about different attacks relating to PII, some of the prominent ones are as follows:

- Identity theft: attacks that lead to loss of sensitive, personal information that can be used as keys to access other information such as financial records. Examples of stolen attributes in such attacks can include stolen Social Security Number, date of birth, etc.

- Social Engineering: attacks that lure victims into sharing their personal data by impersonating or creating a synthetic identity.
- Phishing: attacks that target victims through emails and phone calls to create a sense of urgency in divulging PII or other sensitive information. This attack could be used as a gateway to further attack an organization or for financial incentives.
- Ransomware: attacks that lock up an organization's services through intrusion-based software and hold the company at ransom. Ransomware primarily used for financial gain and can be an induced attack through phishing emails and other malware infected links.
- Malware injection: malicious software that is inserted into a target device without the target user's knowledge. These attacks are then used to gain sensitive information that could again be used as a gateway to further intrude an organization.

THREAT INTELLIGENCE: CONCEPT

Threat Intelligence enables individuals and organizations take a preemptive approach to their cybersecurity defenses as the newfound knowledge arms them with the ability to prioritize defending against attacks, should an attacker take any action against them.

Information characterizing threats are often extremely noisy – there is irrelevant or incomplete data – and ineffective, overwhelming, and is likely in-actionable [1]. However, when an organization can collect, process, and analyze the given information from the sources to understand different attributes about the attacker, such as motives, targets, and patterns, it falls under the field of Threat Intelligence [2].

Threat Intelligence empowers the defending organization by introducing them to new vectors of attack, the attackers' patterns, motives as well as technical knowledge, and enabling them to make better decisions about prioritizations and risk mitigation tactics. Threat Intelligence, in current industry practice, falls under three categories: Strategic, Tactical, and Operational [3]. We utilize a running example, such as company X, to reaffirm the distinctions of threat intelligence categories.

Strategic Intelligence ensures organizations and business understand the executive-level decisions that need to be made based on high-level analysis. Most sources for such intelligence are through open-source inputs, for example, media outlets, online reports, etc. In our instance for company X, the Chief Information Security Officer (CISO) and other executive-level officers find information, such as white papers and other non-technical sources, that give a glimpse of high-level information and trends very useful to make high-level decision.

Additionally, Tactical Intelligence is more granular than high-level analysis as it serves to make technical decisions about the organization's defending systems and whether they can deter the immediate threats. Such intelligence takes inputs from IOCs: Indicators of Compromise comprise of technical, forensic evidence which could indicate an attack or infection [4]. These could include any number of details, such as virus signatures, URLs of malicious web pages, IPs of attackers, etc. Company X's security team leads would often find this information vital. This intelligence would include reports from the company's security vendors to understand where resources would need to focus for prevention and mitigation response.

Lastly, Operational Intelligence answers the immediate questions of who is affected, how are they affected, and what is being used. This intelligence is often utilized

to understand the context on various factors such as motivation, attack vectors, and any other patterns. Enough Operational Intel is gained from learning more about ongoing cyber incidents or any prior incidents an organization has had to face. Daily, company X's Security Operations Center (SOC) would filter incoming data through various feeds and start drilling down more on the true-positive events.

With these categories of intelligence, and given appropriate consolidation of such intelligence, an organization can have actionable data which can be utilized effectively to strengthen defenses through prioritization of risk mitigation tactics, deterrence of initial attack vectors, or overall investing in stronger system security.

INFORMATION SHARING AND ITS FACILITATION

As the every-growing interconnectivity increases, information sharing as part of threat intelligence exchange has become extremely vital. With new knowledge gained about certain attacks from one part of the nation or world, it is imperative that other defending organizations are made aware of such new attacks in timely manner to ensure detrimental effects of such attacks are mitigated, if not deterred.

Often, the idea of information sharing or knowledge sharing in cybersecurity realm is misunderstood [5]. Current industry practices make the organizations reluctant to sharing any proprietary information publicly, which could potentially give advantage to their competitors. However, information sharing can also be divided into the 3 levels of intelligence – Strategic, Tactical, and Operational – as stated by Luiijf et al. [5]. The information shared usually relates to possible incident response steps that can be taken rather than organizational decisions made as part of escalation.

There has been industry exploration into improving cyber security information sharing. Dandurand et al. [14] explored the requirements for the Cyber Security Data Exchange and Collaboration Infrastructure (CDXI). The requirements provided the formalized guidelines for private market sectors and how their data would adhere to controlled multilateral sharing which could be customizable based on the information an organization is comfortable sharing. Further, to make it more versatile, one of the other key requirements for CDXI is to be machine-readable and have a human-friendly view to ensure cybersecurity information is viewable by members of an organization with and without technical knowledge. It gives room for nontechnical stories to come from organizations that do not specialize in the security field, thereby increasing parts of the organization that absorb such information.

Although there are plenty of different anonymization procedures and safe haven policies for private and public information storing, the fluid exchange of information between the United States industries and the US federal government has been rather slow. However, with the rise of digital dependency in the current US infrastructure and the risks they can present [6], the US government had to further facilitate knowledge transfer through incentivized voluntarily information exchange. Under the Obama Administration, the Cybersecurity Information Sharing Act of 2015 was passed to further this agenda [7]. With the law in place, federal government assures more protections to the private industry in exchange for sharing their threat indicators – technical knowledge such as IOCs – and their implemented defensive measures. These protections include protection from disclosure, protection from liability, protections from misuse, etc.

Through such encouragement of knowledge and intelligence sharing, non-profit organizations such as MITRE have stepped up to take advantage of the federal funding and

partnerships between the public and private industries to ensure that such partnerships, through open sharing of such intelligence, aids in a safer cyberspace for industries and nations [8]. Like Luiijf et al. [5], MITRE has implemented a matrix – the ATT&CK Matrix – suggesting lists of possible horizontal movement throughout the incident response for any given cyber incident [9], as seen in Figure 1. The attack usually moves from an intrusion-based attack to exfiltration. MITRE's framework aids the reader in understanding the possible next steps the attacker would take to laterally move in the target system which can create an impact. It also divides each attack into threat tactics, threat techniques, and mitigation tactics. While threat tactic gives an overall picture of the type of attack, techniques describe the more technical details about how the bad actor intends to breach the system. Since the possibility of giving information about vertical response to an incident can be too narrowed due to the different access level controls each organization has, leaning towards impracticality, there are possible issues of exposing proprietary information about business decisions from the public and private sector which should be protected. It should be noted that alerts from the United States CISA currently apply the MITRE mitigation and detection techniques, indicating the matrix is being actively used in private and public sectors as guidelines for incident responses.

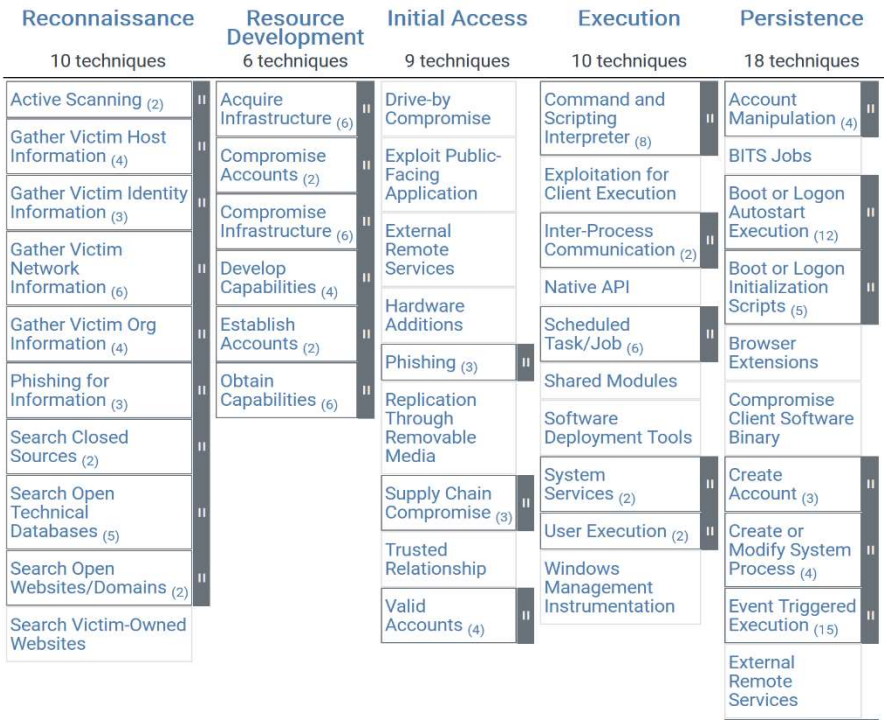


Figure 1: A Snippet from the MITRE ATT&CK framework where cyber incidents are linked to more detail and their lateral incident response tactics [10].

OPPORTUNITIES FROM INFORMATION SHARING FACILITATION

With a rise of information sharing between private industries and the federal sectors, we have seen a surge in information provided through journalism and other media outlets. This information is conventionally classified as Open-Source Intelligence (OSINT): information which is available publicly and is encouraged to be used and shared for the betterment of the cyber communities [11]. There are multiple types of OSINT outlets, and for the purposes of this research, we are focusing on the media outlets. Aside from the aggregated reports released in media, news media also covers different stories shared through mediums such as newspapers, online articles, television, and radios [12]. Other forms of informal sources for OSINT include Long-Form and Short-Form Social

Media Content which includes different threads on cyber incidents through websites such as Reddit and alerts and further news development on social media such as Facebook, respectively. Although OSINT – especially from media – is very effective as part of knowledge sharing, one of the severe limitations is the lack of technical details due to the jargon it introduces, inhibiting regular readers from understanding the context. This, in turn, results in less technical details for defending teams when parsing through the OSINT.

With an easier access to such outlets and artificial attempts to further boost information sharing and promote a sense of transparency, there is opportunity to turn such information into actionable data. The University of Texas's Center for Identity has utilized such open-source intel and created the Identity Threat Assessment and Prediction (ITAP) Model [13]. ITAP utilizes OSINT such as news stories and personal stories to aggregate data on exposure of PII and the market sector from where the attacks have been reported from. Though not actionable data, the ITAP model aims to visualize the patterns and a higher-level analysis by providing Strategic Intelligence and extract vital information from the different stories. ITAP is covered in more detail later and is one of the many examples of how readily available OSINT and other informal sources can be tapped for information related to threat intelligence in any of the three categories described above.

This research focuses on utilizing such sources to provide actionable data which can be added to the knowledge databases of market sector leads who are actively interested in learning more from different outlets of threat intelligence and act on any preventive and mitigation efforts to deter harm.

Chapter 2: *Related Work*

This chapter entails the current work conducted through facilitation of information sharing. We describe the current processes of creating a safer cyberspace and various aspects where they are flawed.

There has been previous academic work in the "blue team" sectors – teams in organization that focus on defending from various cyber threats – that focus on helping organizations understand the different trends and cyber incidents (not including significant cyber incidents, as described by Presidential Policy Directive-41 [15]). Although most resources discussed in the chapter covers work within the United States, some notable related efforts across the globe are acknowledged.

INFORMATION SHARING OUTSIDE OF THE UNITED STATES

Throughout the world, dedicated cyber operations commands of each nation act to ensure that aggregated information is passed down as part of declassified information from the government intelligence. For example, The Australian Cyber Security Centre issues surveys on annual basis that sends out aggregated information about the types, frequency, and impact of reported cyber incidents [16]. Although the report is extremely comprehensive which also includes incidents from different types of OSINT outlets, as discussed in the previous chapter and the type of impact faced by the incident, it fails to provide any data to encourage vigilance for specific market sectors. The survey also does not distinguish between incidents relating to individuals and organizations. Further, the granularity on each incident is ambiguous with no indication of the duration of attack or any countermeasure taken. This, therefore, depicts an unclear picture about the timeline of any incident and any response to it.

On a global collaborative scale, The North Atlantic Treaty Organization (NATO) has attempted to share educational information about the different frameworks – as well as possible mitigation tactics from different attack vectors [17]. NATO shares their educational framework for the purposes of facilitating skill-based information for cyber-security professional all over the world. Since NATO does not entail or cater to one specific nation, the organization does not provide any data on any incidents that pertain to any nation. Furthermore, due to the ambiguity of international laws that are fostered due to lack of common objectives by influencing powers, such as the United States, China, and Russia [18], NATO lacks explicit powers on either side of the cyber security terrain, thereby refraining it from having any concrete methodologies to respond to attack vectors that can be applied in multiple nations, adhering to the nation's set of laws. Although it serves the public with important information to further nurture incoming cyber security professionals by creating technical educational frameworks, as well as aiding in deciphering any international law pertaining to the issue, NATO does not share information that relate to non-state actors.

WITHIN US: FEDERAL LAW ENFORCEMENT

Within the United States, the federal government has established forces in the law enforcement and executive branch, such as The Federal Bureau of Investigation (with Department of Justice) and United States Secret Service, that have dedicated cybercrime branches to keep the domestic organizations and civilian population safe.

FBI's Cyber Investigation team works closely with local law enforcement in its field offices. With the given coverage, individuals can request aid for incidents through FBI's Internet Crime Complaint Center (IC3) [19] while organizations can contact law

enforcement and federal agents as need be. Focusing on the IC3, FBI also aims to release the information collected about incidents that were reported. The Bureau releases certain attributes of the reported incidents such as basic demographic information, estimated financial impact, and types of cybercrimes that occurred [21]. However, like other cyber security centers around the globe, the reports do not provide any mitigation responses as well as market sector specific trends that could indicate patterns for market sector leads as they parse through the reports. Further, FBI admits that due to the report only accounting for reported complaints, only 12% of actual cyber incidents are being captured by the reports [20]. This further undermines the captured trends in the report as compared to other OSINT sources, such as individual media outlets for individual cases.

FBI also utilizes another tool, labeled as iGuardian [22], as an industry-focused cyber intrusion system. It is actively used when law enforcement is involved for an incident involving organization (especially critical infrastructures as defined by CISA [23]). However, since there is no publicly available information available, this research does not relate to the findings of the tool.

Moreover, the federal government also utilizes Secret Service Cyber Investigations to primarily focus on financial market sector and cyber security cases related to it [24]. Secret Service does provide generalized information from their knowledge database on various cyber incidents and how to respond to them, but due to the nature of the cases they are assigned, there is no declassified report of the trends and any other aggregated report available online for the general populace to view. The media outreach team of the Secret Service does release information about recently concluded cyber investigations, but do not reveal all the information needed for further prevention of such incidents.

Additionally, US Department of Justice also aids in releasing reports to address the different cybercrimes trends and statistics, through the Bureau of Justice Statistics (BJS) [40,41] in aiding the US populace understand the different demographics of the victims involved in such crimes. However, the intention of such reports is to inform the public of annual trends and not to make any decisions. The reports provide a general cause of these cyber and information crimes, such as lack of anti-virus software, and derive the percentage of incidents caused by it. However, they do not provide any recommendation – implicit or explicit – to deter such attacks as a member of any organization or individual. The primary focus of BJS reports is to share Justice Department's information database in statistical manner that citizens can further analyze and make decisions with, as part of Strategic Intelligence.

Overall, the federal reports and media press released by federal law enforcement organizations provide data to the public and organizations that is statistically interesting. Also, the data provided is reactive rather than preventive: information from the shared data cannot be used for any prevention, but rather results of action that are too late.

WITHIN US: CISA ALERTS

Although the reports provided aggregated yet no actionable data, the Cybersecurity and Infrastructure Security Agency provides time-sensitive and actionable alerts for the general public as well as the organizations to view and digest as they see fit [25]. CISA alerts follow the MITRE ATT&CK framework analysis (discussed in the previous section) that ensures a mitigation response as well as detection techniques are easily understandable due to easy access to the ATT&CK framework. Figure 2 depicts one of the recent alerts from the ATT&CK framework. The framework aids in understanding the impact of the

attack, possible detection approaches, as well as structured incident response to it. Further, CISA also includes the market sector of interest with their alerts. For instance, CISA would title alerts related to educational institutions with the keyword “Education”, as can been seen with alert AA20-345A, that intuitively lets the reader focus on their market sector of interest.

Although the alerts pushed by CISA are of industry and organizational interests, the agency does not use openly available information that pertains to incidents to domestic and local cyber incidents. With the federal government focusing on incidents that are of national security interest, actionable alerts would not cover domestic incidents such as social engineering or small ransomware cases as compared to local media. The coverage, therefore, is limited to alerts that involve advanced persistent threats and nation state actors that attempt to jeopardize the cybersecurity infrastructure for critical or large-scale organizations and not on individual bases.

CISA has observed Chinese MSS-affiliated actors using the techniques in table 1 to gather technical information to enable cyber operations against Federal Government networks (*Technical Information Gathering* [TA0015]).

Table 1: Technical information gathering techniques observed by CISA

MITRE ID	Name	Observation
T1245	Determine Approach/Attack Vector	The threat actors narrowed the attack vectors to relatively recent vulnerability disclosures with open-source exploits.
T1247	Acquire Open Source Intelligence (OSINT) Data Sets and Information	CISA observed activity from network proxy service Internet Protocol (IP) addresses to three Federal Government webpages. This activity appeared to enable information gathering activities.
T1254	Conduct Active Scanning	CISA analysts reviewed the network activity of known threat actor IP addresses and found evidence of reconnaissance activity involving virtual security devices.

Figure 2: A snippet from the CISA Alert AA20-258A showing MITRE ATT&CK implementation, facilitating easier diffusion of information between CISA and the public [26].

WITHIN US: ACADEMIC WORK IN INFORMATION SHARING

Aside from the federal government, other organizations are also involved with the community through information sharing and helping in creating better defenses for everyone in the cyberspace.

There has been academic exploration on how to integrate the ATT&CK framework when supplying IOCs and its related information. From technical viewpoints, Farooq and Otaibi [37] depict multiple examples of utilizing machine learning (ML) and associating ML use cases with the ATT&CK framework, notably for the Exfiltration detection techniques. The authors present K-Means clusters and relate them to a quadrant that is based off the Exfiltration techniques to detect user activity and any potential signs for malicious software injections or data leakage in forms of Command and Control, covert channels, etc. The work provides detail in mimicking the detection techniques for any organization's SOC although it does not provide any testing criteria or compare accuracies from open databases. However, such information sharing on detection is exceptionally important to integrate with industry standards of attack techniques and behavior because of the novel cases seen by organizations, enabling their SOCs to detect IOCs attacking their organization.

Similarly, there has been previous work in surveying current cyber-attack emulators such as Red Team Automation [39] with the ATT&CK framework in sharing more information from the attacker's perspective [38] where the authors assess the highlights of its (and other simulators') scripts while looking at the implementation based on the ATT&CK mapping. Through the surveys, the audience gets more information about utilizing best emulators to create scenarios and test out their abilities for deterrence and mitigation tactics based on the ATT&CK framework.

With more open news outlets (as part of OSINT), such as Twitter and 0day.today, non-federal organizations have also been able to aggregate the data coming in for the purposes of information sharing that is not regulated by the government. For instance, The University of Texas's Identity Threat Assessment and Prediction reports [27] utilizes news stories and other open-source information gathering outlets to collect information about PII related cyber incidents. The ITAP model can capture large numbers of incidents as raw data and parse through to understand the vulnerabilities exploited, data that was breached, and steps taken by the bad actor to achieve their goal. ITAP accounts for cases after the year 2000 and can analyze trends in the types of cyber incidents as well as different sectors. The report further details the findings and visualizes it into different categories and trends such as impact of loss, demographics of victims, etc.

Various other academic works use the ITAP Dataset to further research the PII assets, their risk of exposure, protection strategies, and minimizing risk [52-65].

Like we have seen in previous work, the ITAP report is published annually with all the aggregated information about incidents from the past year. Though it aids in visualizing the trends and patterns of cyber incidents in various market sectors, it fails to provide the information in a timely manner that can be incorporated by individuals and organizations alike and attempt to take any preventive actions to protect themselves from the attack. Moreover, with the given information, ITAP is not able to provide any explicit recommendations for prevention measures.

WITHIN US: NON-ACADEMIC WORK IN INFORMATION SHARING

Like ITAP, Verizon releases data breach reports with incidents that are related to its forensic and intelligence operations [28]. The incidents that are explained in the annual

Verizon report are shaped in the VERIS framework [29] – which is similar to the ATT&CK framework as described above – that standardizes the information extracted. Verizon's report is very comprehensive because it can capture concrete steps, threat patterns, frequency, and the data compromised. Although the report does not focus primarily on PII data, the information capture and visualized can be of great aid to the public and market sector leaders in efforts of making their defenses more resilient. It should be noted that though they provide the general efforts for increasing defenses, the granularity is lost and not viewable for each incident captured. The report, based on the trends and other factors, releases general recommendations for security effort, but does not give any recommendation at an individual incident basis or even market sector basis. This, included with the fact that the data and trends are not provided on more frequent basis other than annual reporting, undermines the overall effort in utilizing the open data.

Crowdstrike's Global Threat Reports further details the specialized 2020 overview by focusing on the surge of new trends such as COVID-19 vaccine scams, data extortion, etc. [36]. With the 2020 pandemic, there has been a surge of remote workers due to the concerns for safety. Unfortunately, this also led to a high number of attacks due to remote authentication, the panic about the pandemic, and other uncertainties that were exploited by bad actors. The report further mentions how nation state actors played a role in targeted intrusions and what the reported adversaries were attributed to them. However, a significant contribution for intelligence sharing for cyber-defense sector comes from the report's IOCs of different remote vulnerabilities. Through the collected intelligence, Crowdstrike can inform its audience about different stages of repetitive credential acquisitions as well as generate recommendations on how to protect an organization from it and all the other reported threats. Though generalized, the recommendations mimic

various mitigation techniques as seen in CISA alerts and MITRE ATT&CK framework, indicating versatility and easy application in the organization. However, the aggregation of all the collected data and creation of the report failed to deliver actionable intelligence to such organizations in timely manner. Though the intelligence was collected throughout the year, no recommendation or any other intelligence was publicly posted as part of the threat report in weekly or monthly manner. Delayed information always leads to a reactive response rather than proactive response.

THREAT INTELLIGENCE COMPANIES

There is a plethora of companies that address this domain issue of threat intelligence in forms of business models. Companies like Crowdstrike, IBM X-Force, Virustotal, etc. [30,31,32] have business models oriented towards gathering threat intelligence in all formats followed by digesting, analyzing, and reporting the information in timely manner to the organization.

Features	Free Version: Virustotal	Paid Version: Virustotal
Search based on IOCs	Yes	Yes
99% uptime for automation API	No	Yes
Threat intelligence and recommendation notifications	No	Yes
Behavioral and threat indicator activity for malware	No	Yes

Features	Free Version: IBM X-Force	Paid Version: IBM X-Force
Search based on IOC	Yes	Yes
Access machine-readable actionable intelligence	No	Yes
Early warning threat notification	No	Yes
Threat Intelligence Reports	No	Yes

Table 1: Tables show a list of features for Virustotal and IBM X Force, respectively. It compares the features offered as part of their free services versus what the customer misses out by not opting in paid subscriptions [33]. Table 1 is not an exhaustive list of the features available on each platform.

Table 1 shows a non-exhaustive list of features that are offered by these threat intel services. It should be noted that the enterprise (paid) subscription comes with a lot more features than listed in Table 1. With the current subscription costs of such services being closer to ten thousand dollars per annum [34], smaller organizations can get isolated as they likely do not have the same budgets for cybersecurity as bigger organizations. Further, the budgeting of smaller enterprises tends to focus more on endpoint protection for reactive response rather than intelligence gathering for a proactive approach, as advised by the framework put out by CISA [35], leading to intelligence gathering be of lower priority and risk smaller organizations be a lucrative target for bad actors.

With all the different efforts described – from around the globe to specific US solutions – they all fall short in their ability to provide an easily accessible platform or solution that enables organizations of any size to access the current trends and intelligence to understand emerging threats in their sector, as well as understand the appropriate response to prevent bad actor from intruding in their system. I-WARN aims to rectify that through providing such intelligence in timely manner thereby openly assist in making our virtual space safer.

Chapter 3: *System Overview*

This chapter covers the technical details for I-WARN. We will discuss all aspects of the backend logic as well as frontend integration.

SYSTEM OVERVIEW

I-WARN is designed to be a webpage that can be accessed by any device connected to the internet. We use Python 3.7 for the backend logic, ITAP dataset as input to the system, and Python Flask [42] coupled with HTML and JavaScript for the front end. More aspects of each part of the project are detailed below.

On a high-level overview, The ITAP dataset is fed into a parser script where it is parsed to extract information elements, such as steps or inputs used by attackers during an incident, for the system to map a story to a specified ATT&CK threat tactic from the matrix through a scoring system. We discuss why we used ATT&CK matrix later. Once the information is collected, we create a score for each story to understand the more likely threat tactic utilized based on the inputs and steps taken by the attacker during an incident. Lastly, when the scores are created, we further extract the market sector and send over the details to an automation script for it to create a possible list of mitigation tactics.

From there, the output is then fed into the Graphical User Interface (GUI) where it can display descriptions, mitigation tactics, and top threat tactics for each story. There are other features such as the CISA Alert feed also available from the GUI. Figure 3 gives a high-level overview of the whole system to further visualize I-WARN.

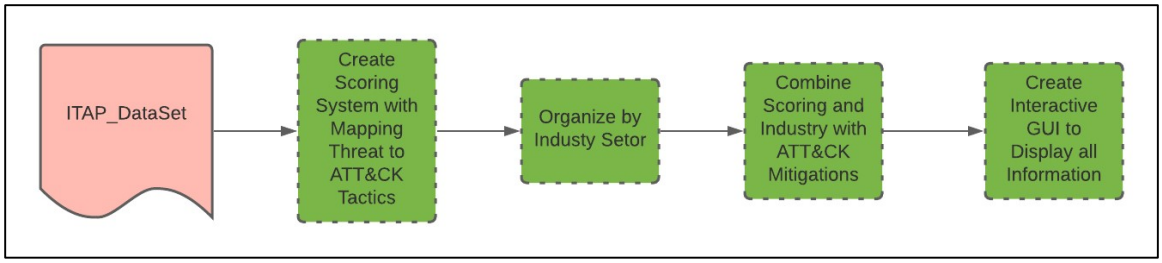


Figure 3: High-level overview of the system where the lifecycle of each story – from ITAP dataset to the frontend – is shown.

ITAP DATASET

Each story in the ITAP dataset contains the inputs used by the attackers, the outputs of what the attackers were able to exfiltrate or utilize, and the steps they took to exploit vulnerabilities, conduct crimes of theft, fraud and abuse then ultimately to produce a wide range of consequences. Aside from such facts, every story also contains the resources used to conduct the attack, general biographical information about victims, any attribution to the attacker, and deployed countermeasures. Gathering of all the information indicates a very thorough study of each story and reaffirms every piece of intelligence which can be extracted.

Currently, the ITAP dataset contains approximately 6000 stories gathered from the OSINT outlets, captured between the years 2000 and 2020. These stories are manually modeled[1]. Most of the stories contained in the ITAP dataset are related to identity-related crimes such as identity theft, social engineering, and phishing. The ITAP dataset also contains attacks such as Ransomware as they are related to further attacks caused by social engineering and phishing. Table 2 shows a snippet of the ITAP information contained for each story.

[1] We are currently exploring machine learning options to automate modeling stories.

Inputs	Outputs	Steps	Loss Incurred	Countermeasures
Employee Credentials Stolen, Malware Injected, Password, Username	Bank Account Information, Bank Account(s) Compromised, Name, Payroll System Breached	Analyze, Infect, Breach, Steal, Transfer	Emotional Distress	[REDACTED] became aware of the attempt and immediately cancelled the fraudulent direct deposit accounts. The affected employees were also notified.
File(s) Copied without Authorization, Organization Proprietary Information Stolen	Customer Information, Organization Proprietary Information	Transfer, Steal	Emotional Distress, Intellectual Property	Charged with theft.
Malware Injected	Credit Card Information, Personally Identifiable Information (PII)	Breach, Infect, Acquire	Emotional Distress	malware removed, security measures enhanced, victims notified
Employee Access to Database Misused, Employee Login Credentials	Address, Date of Birth, Name, Social Security Number, Victim(s) Surveilled	Abuse, Surveil	Property	victims notified
Victim(s) Selected	DDoS Attack Initiated	Coordinate, Act Upon	Emotional Distress, Financial, Property, Reputation	[REDACTED] was sentenced to 36 months in probation, 60 hours of community service, $110,932.71 in restitution

Table 2: A snippet of the ITAP dataset with inputs, outputs, and steps taken by the bad actor. It also depicts the loss incurred by victims as well as countermeasures deployed. Aspects of counter measure with PII have been redacted. Information contained in the table for each story is not exhaustive.

MAPPING THREATS TO I-WARN

We start the discussion of mapping logic with the utilization of MITRE ATT&CK framework [10]. Currently, ATT&CK framework is being utilized by actionable alerts provided by CISA [25], as well as by multiple non-federal information sharing [37,39]. The ATT&CK framework works well because of its simplicity in visualizing the lateral movement of possible attacks. With techniques, the ATT&CK framework also provides previous history of such uses and other attributional details, which can be used to further investigate by the organization's security team. There are also possible detections provided for ways to assist blue teams in understanding how the attacker plans to use a point of entry and how they can look for IOCs. Mitigation tactics are also incorporated with each technique and helps the reader understand what steps can be taken to either prevent the attack at point of entry or mitigate any potential damage. With such eclectic set of information provided – and regularly updated – as part of OSINT, it was easier for us to integrate the ATT&CK framework in our work. Moreover, the relevance of the ATT&CK framework was also a key reason for us to use it. With the current US government alerts coming through the ATT&CK framework integration and given the fact that we aim to share information primarily in the US, it was vital to integrate our work with this current infrastructure.

Next, we designed a logic map based on the keywords used in the ITAP dataset. The inputs and steps used in each story, as described in Table 2, give an overall picture about the incident that has taken place. Given that these stories were not entailing a lot of technical information, we had to manually parse through the keywords to associate them with threat tactics established in the ATT&CK framework. Since the stories are generalized, we decided to not attempt to not focus on threat techniques, but rather keep it

broader with threat tactics to avoid any risk of overfitting the ITAP dataset. Table 3 shows us the manual logic used for mapping keywords to threat tactics in the ATT&CK framework.

To ensure keywords are captured correctly, we grouped many inputs to the proper keyword, reinforcing the logic as well as making it more simplistic when mapping to threat tactics. For example, we grouped inputs such as “Twitter”, “Facebook”, “social media” as Social Media Involvement. We collected and grouped all the ITAP inputs into 20 keywords, as shown in Table 3.

As mentioned before, the stories captured by ITAP are part of OSINT, thereby eliminating extensive technical details that can be incorporated in each. Given the stories are manually parsed and have been fully extracted, some contents of stories lead to ambiguity when it comes to pinpointing the exact threat tactic utilized by the bad actor. To counter that, we created a scoring system which assists in pinpointing the “most likely” threat tactics used. Since the generalization is something inevitable with OSINT (particularly media outlets) we overlap a few keywords – as seen in Table 3 – and give them a likely score of the possible threat tactics used. This ensures we can create a coverage that is adaptable as more stories are added, without risking to narrow results based on the specified 6000 stories.

Once the ITAP dataset was parsed and each story is given a score for the most likely threat tactics used, we prune the MITRE matrix to eliminate unnecessary threat techniques, prior to providing mitigation tactics. Since the ITAP dataset is comprised of OSINT from media outlets, all the technical details described in the ATT&CK framework cannot be mapped to the stories. To eliminate this issue, we created a dictionary – part of which is shown in Figure 4 – to take out extremely technical threat techniques. We also eliminated

threat sub-techniques that stemmed from the said techniques. This way, we can filter out mitigation tactics that are not applicable to techniques which are never addressed in the ITAP dataset. This is one the limitations of this work which will be discussed in later chapters. With the unwanted mitigation tactics and threat techniques eliminated, we map the remaining mitigation tactics to each threat tactic, and story, that generalizes all the possible steps an organization can take to limit or prevent any loss potentially incurred due to the attack.

ORGANIZE MARKET SECTOR

The ITAP dataset contains market sectors where each incident took place. However, due the specification provided in the ITAP dataset, we further generalized the market sector to aid in understanding of general trends. For instance, we grouped together market sectors containing the keyword "health", "hospital", "clinics", etc. as healthcare. We grouped together all the market sectors of ~6000 stories into 12 market sectors. 11 out of 12 market sector keywords are readily mappable to known classification of market sectors, such as healthcare, religious organizations, etc. Out of the 11, 7 are classified to be part of the CISA Critical Infrastructure Sectors [23]. The remaining four are known sectors: education, religious organizations, hotels, and travel. The 12th one is meant to be miscellaneous – market sectors and companies that are not well known or do not fit in a generic sector – such as anonymous organizations, various companies grouped, clubs, etc. We classify organizations as miscellaneous if they cannot be grouped into the 11 other classifications. This information is collected and then passed on to be viewed on the GUI as discussed later in this chapter.

This separation of market sectors ensures that leaders of specified market sector can view generalized trends in their fields as well as explore the stories specific to their market sector. This would ensure they are able to filter out any noise related with other market sectors and take reactive or proactive measures based on the news, threat tactics, and mitigation suggestions.

```
technique_to_exclude_dict["Command and Control"] = []
technique_to_exclude_dict["Exfiltration"] = ["Data Transfer Size Limits", "Exfiltration Over C2 Channel"]
technique_to_exclude_dict["Impact"] = ["Firmware Corruption", "Inhibit System Recovery", "Resource Hijacking", "Service Stop"]
```

Figure 4: A snippet from the code showing the dictionary that is used to eliminate unnecessary techniques which are not seen in the ITAP dataset due to the high technical knowledge required.

Threat Tactics	ITAP Input used	ITAP Steps Used
Reconnaissance	“Broken Into", “Phishing”, “Social Media”	“Analyze”, “Surveil”, “Break Into”, “Misplace”, “Mismanage”
Resource Development	"PII/Credential Stolen", "Synthetic Information"	"Impersonate", "Compile", "Lie", "Communicate", "Alter"
Initial Access	"Synthetic Information", "Devices mishandled", "Security vulnerability/Mismanage", "Phishing/Spear-Phishing", "PII/Credential Stolen"	"Request", "Send", "Infect", "Acquire", "Mismanage", "Impersonate", "Malfunction", "Misplace", "Communicate"
Execution	"Malicious Link", "Malware", "Ransomware"	"Breach", "Infect", "Coordinate"
Persistence	"Access Misuse"	"Abuse", "Create", "Activate"
Privilege Escalation	"Access Misuse"	"Abuse"
Defense Evasion	"Access Misuse"	"Conceal"
Credential Access	"Security vulnerability/Mismanage", "Devices Mishandled"	"Steal", "Record"
Discovery	NONE	NONE
Lateral Movement	NONE	NONE
Collection	"Audio/Visual Involvement", "Removable Media", "Email Scam"	"Record", "Discover", "Find"
Command and Control	NONE	NONE
Exfiltration	"Removable Media", "Transfer"	"Inflict Punitive Measure", "Upload", "Steal", "Expose", "Sell", "Transfer", "Leak"
Impact	"Ransomware", "DDOS", "Video Altered"	"Disable", "Destroy", "Block", "Deactivate", "Send", "Request"

Table 3: Table shows all the keywords from ITAP dataset used to create the scoring system. All inputs were grouped prior to mapping them to the threat tactics. More information about the overlaps can be found here: Link to Logic Map.

COMBINING EXTRACTED INFORMATION

Once the ITAP dataset is completely parsed and we successfully extracted market sector, we then combine all the information with ATT&CK mitigation tactics. Each threat tactic is linked with a list of mitigation tactics as recommended by the ATT&CK framework which are then grouped with each granular story.

Since each story extracts top three threat tactics used in the incident, and each threat tactic has a mitigation tactic list linked to it, we attach the lists of these mitigation tactics which are associated with the threat tactics. However, for brevity, we only display the list for top threat tactic in each story. Displayed mitigation tactics are then hyperlinked with the MITRE website and displayed for the reader, further described later in the chapter.

ADDITIONAL FEATURES

In addition to the mapping and displaying of the stories and its associated mitigation recommendation from the ATT&CK framework, we also incorporate other, emergency alerts, such as CISA [25] to the GUI. Because the CISA alerts are published ready and integrated with the MITRE ATT&CK framework, adding the alerts was a vital feature to incorporate in I-WARN as it then offers itself as a hub to more intelligence – governmental and non-governmental alerts – that organizations can utilize from one location. As part of future works, we aim to expand and incorporate other open knowledge sharing systems as well.

Other additional features are further discussed as part of future works in later chapters.

GUI

We use Flask for I-WARN due to the increased dependency of a web framework and the ease it offers to upload the project on platforms, like Amazon Web Services, when we are ready to publish. With Flask, we can set up our localhost to a specified port and view the GUI ourselves. Other debugging tools offered in the development environment also make it a lucrative choice.

Figure 5 shows us the main homepage that a I-WARN user sees. We see the tabs of each market sector, as well as CISA alerts. Further, the homepage has an interactive pie chart that shows the current number of cases for each market sector. The pie chart is created using HTML and embedded JavaScript through Google charts as well as other sources for navigation bars [43, 66, 67] and is adaptable to more market sectors, should they be added in the future.

Additionally, there is a table to show the most common threat tactics being utilized in each market sector, part of which is shown in Figure 5. On the backend, we calculate the frequency of each threat tactic in each market sector and list out the most frequent ones used for each market sector. We hope that these show the market sector leads common trends occurring in their fields and can act in preventing being a target.

Diving deep into each sector, the stories are divided by the story number – which is a simple index that can be replaced with more specific names – followed by the top three threat tactics likely used in the story. These tables, like the homepage, are interactive [66] and can be clicked to get more information. When clicked, each story shows the description of the threat tactics in use, as well as the list of mitigation tactics for the top threat tactic (Figure 6). We create a list in the backend and hyperlink it to the MITRE website in case the reader wants more information about each mitigation tactic and how it relates to

different threat techniques, as seen with the blue text in the second picture (Figure 6). We also conduct a frequency analysis on all the mitigation tactics to give a priority mitigation suggestion based on the mitigation tactic which covers the most threat tactics used in each story, shown in Figure 6. Lastly, we provide an interactive table for the CISA alerts as well, as seen in Figure 7. The alerts are based on the current information issued by CISA regarding any threats they deem of interest, as well as the mitigation and detection tactics. Since the alerts are already integrated with ATT&CK framework, we do not hyperlink anything to the MITRE website. Each row gives a detailed description, detection, and mitigation suggestions for the alert. All the details are parsed through the XML file, sent through the CISA RSS feed.

As more features are developed in near future, we will update the GUI as need be.

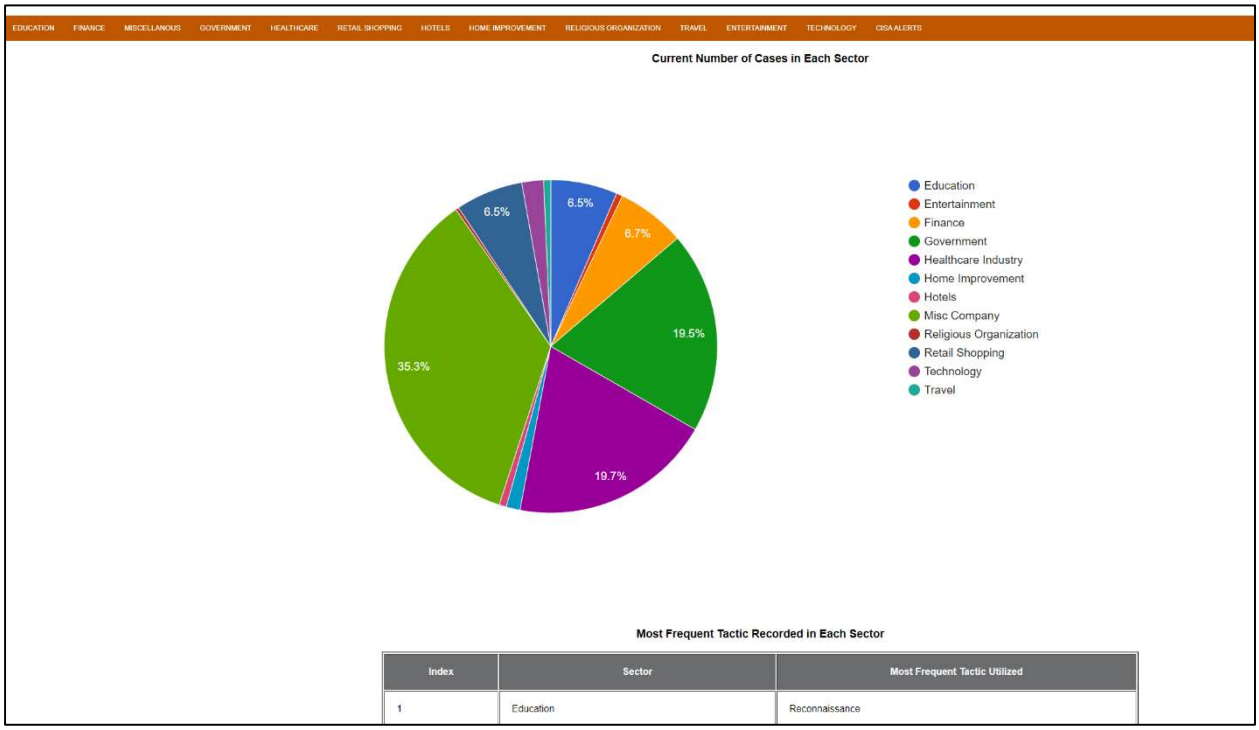
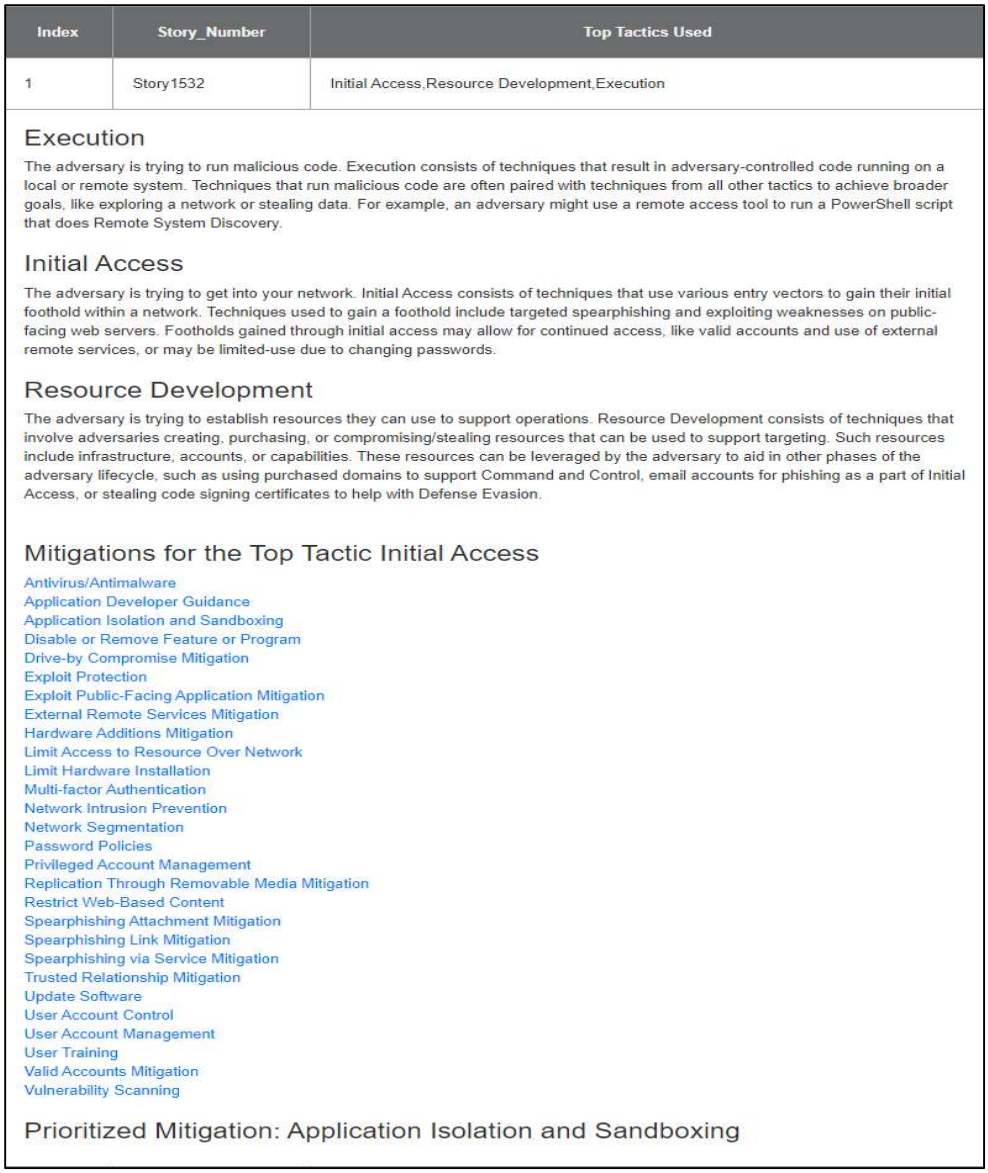


Figure 5: Snippet from the GUI. The first one shows the webpage, as well as the pie chart showing the number of cases in each market sector. The education trends for threat tactics can also be seen, based off the current ITAP dataset.



Index	Story_Number	Top Tactics Used
1	Story1532	Initial Access,Resource Development,Execution

Execution

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Initial Access

The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Resource Development

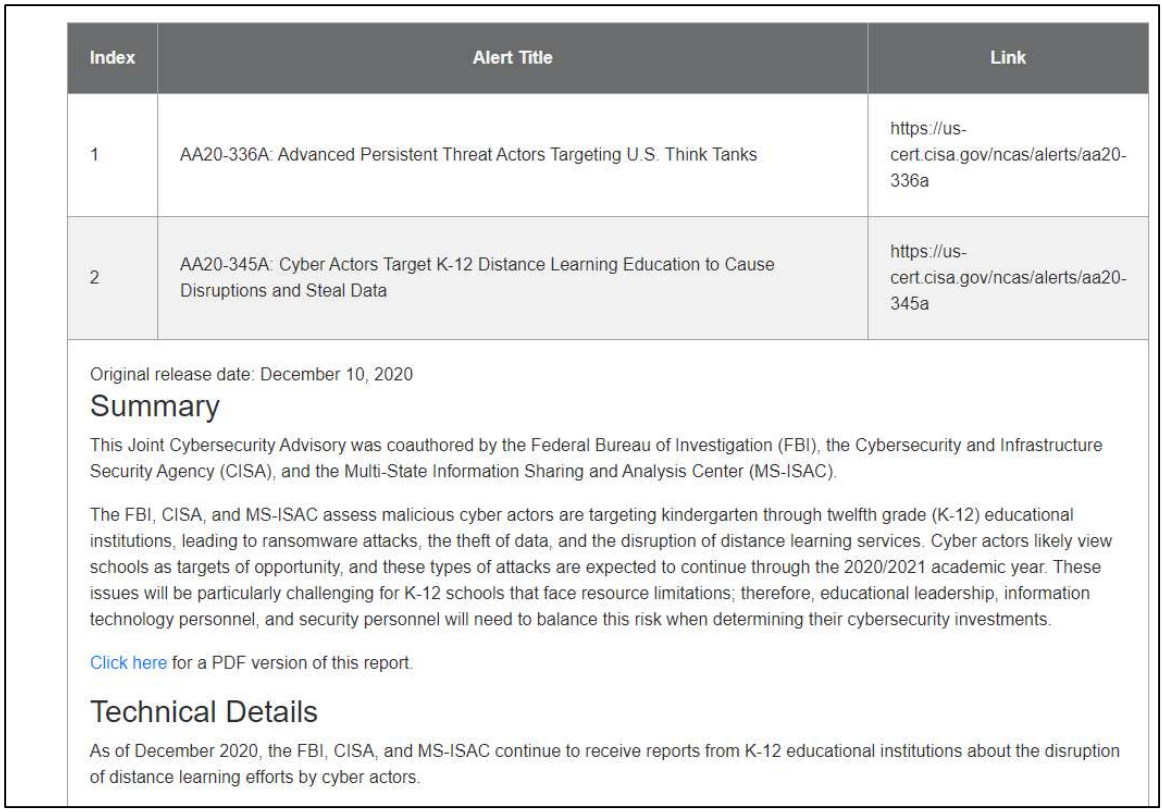
The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

Mitigations for the Top Tactic Initial Access

Antivirus/Antimalware
Application Developer Guidance
Application Isolation and Sandboxing
Disable or Remove Feature or Program
Drive-by Compromise Mitigation
Exploit Protection
Exploit Public-Facing Application Mitigation
External Remote Services Mitigation
Hardware Additions Mitigation
Limit Access to Resource Over Network
Limit Hardware Installation
Multi-factor Authentication
Network Intrusion Prevention
Network Segmentation
Password Policies
Privileged Account Management
Replication Through Removable Media Mitigation
Restrict Web-Based Content
Spearphishing Attachment Mitigation
Spearphishing Link Mitigation
Spearphishing via Service Mitigation
Trusted Relationship Mitigation
Update Software
User Account Control
User Account Management
User Training
Valid Accounts Mitigation
Vulnerability Scanning

Prioritized Mitigation: Application Isolation and Sandboxing

Figure 6: The image shows the granularity of each story, divided by each sector. Each story has the description for top threat tactics used as well as hyperlinked mitigation suggestions, followed by the priority mitigation suggestion.



Index	Alert Title	Link
1	AA20-336A: Advanced Persistent Threat Actors Targeting U.S. Think Tanks	https://us-cert.cisa.gov/ncas/alerts/aa20-336a
2	AA20-345A: Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data	https://us-cert.cisa.gov/ncas/alerts/aa20-345a

Original release date: December 10, 2020

Summary

This Joint Cybersecurity Advisory was coauthored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The FBI, CISA, and MS-ISAC assess malicious cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services. Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year. These issues will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.

Click here for a PDF version of this report.

Technical Details

As of December 2020, the FBI, CISA, and MS-ISAC continue to receive reports from K-12 educational institutions about the disruption of distance learning efforts by cyber actors.

Figure 7: Image shows the CISA alert tab that also shows how much information each alert carries, and how the technical details can be mapped with MITRE ATT&CK matrix.

Chapter 4: *System Testing*

In this chapter, we cover the qualitative testing for I-WARN by comparing it to the current delivery of publicly available mitigation systems.

To ensure that our system stands as a functional intelligence sharing platform, we observe different platforms that are advertised as knowledge sharing systems and compare them to I-WARN in terms of information content, ease of access, etc.

Given that there are different platforms utilized to disperse information, we divide our efforts into observing formal and informal systems. We define formal systems as dedicated webpages and portals that primarily serve to inform the public about cyber security incidents and their related information. Informal systems utilize other platforms (such as Twitter) to inform the public about incidents as well, however, do not contain similar amounts of information as formal systems. For instance, a government dedicated cyber security team would have a dedicated, formal webpage for such use whereas a blogpost for computer enthusiasts may occasionally post some information related to an incident. Table 4 summarizes the different systems and how they compare to I-WARN. We further detail these differences later in the chapter. We compare these systems with I-WARN through the delivery style – how formally or informally a system posts information – followed by target audience. We also observe the general time it takes for an incident to be updated for these systems and if they further post any mitigation tactics related to the incident. Lastly, we compare their input sources with our I-WARN's ITAP dataset as well.

System	Delivery Style	Target Audience	Time of delivery	Mitigation Recommendation?	Input Source
Formal Platforms					
CISA	Formalized; dedicated webpage	Large businesses and organizations	Average: alerts need more time due to interest of national security	Mitigation recommendation pulled from MITRE ATT&CK framework	Intelligence agencies, private organizations
ACSC	Formalized; dedicated webpage	Government, large and small businesses, individuals	Average: alerts need more time due to interest of national security	Generic mitigation tactics, linked mitigation with CISA and other governmental agencies	Intelligence agencies, private organization collaboration
CIS	Formalized; dedicated webpage	Large businesses and organizations	Average: inputs are detailed and need time to be sourced	Combination of specified mitigation tactics and integration with MITRE ATT&CK framework	TLP White alerts, CVEs, other formal systems
Informal Platform					
Twitter	Informal: a social media platform used to reach larger audience	Businesses and individuals	Instantaneous: alerted as soon as identified	No specified mitigation tactics	Cyber security researchers, journalists, individuals
Cyware	Informal: curated webpage that combines different alerts	Businesses and individuals	Fast: alerted as soon as webpages update	No specified mitigation tactics	Different sources and webpages
I-WARN	Formalized; dedicated webpage	Businesses, organizations, and individuals	Fast: alerted as soon as ITAP database updates	Mitigation recommendation pulled from MITRE ATT&CK framework	Open-Source Intelligence (news, media, etc.)

Table 4: Different systems and how they compare with I-WARN.

FORMAL SYSTEMS

We observe various formal systems that are used to deliver notifications about OSINT. This includes publicly available intelligence, as well as white reports from organizations.

Cybersecurity and Infrastructure Security Agency (CISA): CISA, as described in Chapter 2, is the United States federal resource for alerting the public about cybersecurity incidents and related mitigation response. Through federal resources, they focus on incidents that are of national security interest as well as any incidents that target the Critical Infrastructures [23]. CISA collaborates with multiple partners in the federal and private cyber watch sectors to collect information.

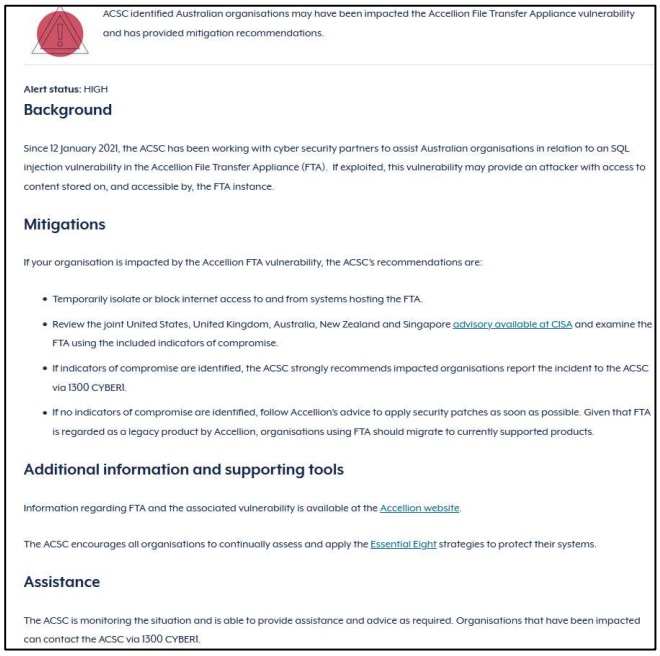
With the various integrations that I-WARN already has established, CISA is a good comparison. As seen in Figure 2, CISA alerts regarding persistent threats that endanger Critical Infrastructure Services comprise of the background of the alert, detection, and mitigation responses – all of which are extracted from the ATT&CK framework. Comparing the CISA alerts to Figure 5, we see that I-WARN derives all its information sharing content from the CISA alerts.

Because each story is extracted from media outlets, I-WARN does not concern itself with given explicit background on each story under the assumption that an extensive coverage of the story has already been done. We plan on adding hyperlinks to each story as part of our future work. Looking at detection and mitigation tactics, I-WARN provides mitigation responses with the links to MITRE mitigation description for the reader to better understand how the mitigation tactic is integrated in their system. The links also serve as a bridge to further investigate what threat techniques are said to be mitigated from the recommendation. Because of the ease of access to the detection and mitigated techniques,

I-WARN compares well with CISA alerts because of the content they both share. Any reader should be able to get in-depth information about cybersecurity alerts available through media outlets through I-WARN in similar fashion of alerts of national security interest through CISA.

Australian Cyber Security Centre (ACSC): We look at the Australian Cyber Security Centre alerts [44] as they annually release reports, seen in Chapter 2, to ensure their citizens and organizations understand cybersecurity trends and take general mitigation steps. Using their governmental resources and private partnerships, ACSC can monitor and collect information about various cyber threats. ACSC also allow citizens to directly complain about cyber incidents that are also registered in their system. Their alerts cater to various sectors such as government organizations, small business, and even individuals.

From Figure 6, we observe that ACSC – like CISA – releases a brief description about the cybersecurity alert as well as mitigation response. Although it does not directly relate to the ATT&CK framework, the mitigation responses are guidelines to review for Indicator of Compromises and recommendation to prevent system intrusion. It should also be noted that the alerts common for Australia and the United States mimic the same mitigation responses and often ACSC would recommend reading the CISA mitigation tactics, as seen in Figure 6. Like ACSC, I-WARN ensures that the mitigation tactics are granular to each story and are hyperlinked to more details, so that they can be further understood by following the links.



ACSC identified Australian organisations may have been impacted the Accellion File Transfer Appliance vulnerability and has provided mitigation recommendations.

Alert status: HIGH

Background

Since 12 January 2021, the ACSC has been working with cyber security partners to assist Australian organisations in relation to an SQL injection vulnerability in the Accellion File Transfer Appliance (FTA). If exploited, this vulnerability may provide an attacker with access to content stored on, and accessible by, the FTA instance.

Mitigations

If your organisation is impacted by the Accellion FTA vulnerability, the ACSC's recommendations are:

- Temporarily isolate or block internet access to and from systems hosting the FTA.
- Review the joint United States, United Kingdom, Australia, New Zealand and Singapore advisory available at CISA and examine the FTA using the included indicators of compromise.
- If indicators of compromise are identified, the ACSC strongly recommends impacted organisations report the incident to the ACSC via 1300 CYBER1.
- If no indicators of compromise are identified, follow Accellion's advice to apply security patches as soon as possible. Given that FTA is regarded as a legacy product by Accellion, organisations using FTA should migrate to currently supported products.

Additional information and supporting tools

Information regarding FTA and the associated vulnerability is available at the Accellion website.

The ACSC encourages all organisations to continually assess and apply the Essential Eight strategies to protect their systems.

Assistance

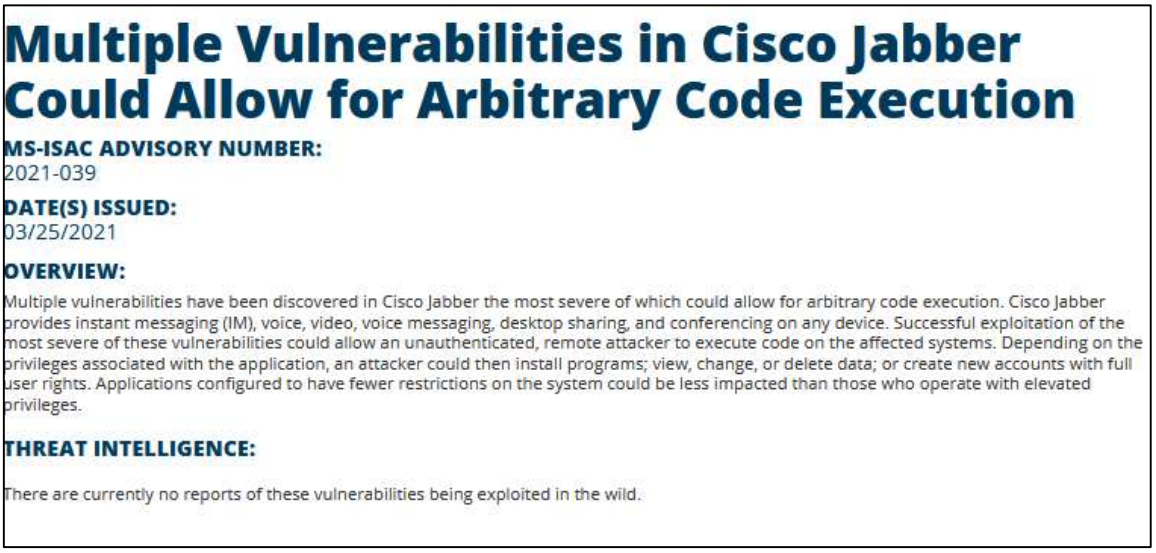
The ACSC is monitoring the situation and is able to provide assistance and advice as required. Organisations that have been impacted can contact the ACSC via 1300 CYBER1.

Figure 8: Snippet from an alert posted by the ACSC [36] that shows the main components of these alerts: background, mitigation tactics, and additional information. It is also interesting to see a reference to CISA as part of their mitigation response to understand more about the given IOCs. We compare the alert to I-WARN and conclude that the content and style of delivery is similar.

Center for Internet Security (CIS): Lastly, we compare I-WARN to non-government formal systems such as the notification system of Center for Internet Security (CIS) [45]. A snippet of CIS's alerts (Figure 7) indicates each alert is taken from CISA Traffic Light Protocol (TLP) White sources[2]. TLP White, according to CISA [46], indicates that the information shared is of public use and sharing with anyone, including any nation state, is permitted. CIS uses such sources to populate their alerts and use a similar fashion of alerting the public as recommended by CISA. One of their primary sources are

[2] This is based off the free alerts provided CIS. I-WARN does not compare itself to CIS subscription alerts as we do not have access to those.

advisories issued by Common Vulnerabilities and Exposures (CVE) – records stored by MITRE.



Multiple Vulnerabilities in Cisco Jabber Could Allow for Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER:
2021-039

DATE(S) ISSUED:
03/25/2021

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco Jabber the most severe of which could allow for arbitrary code execution. Cisco Jabber provides instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing on any device. Successful exploitation of the most severe of these vulnerabilities could allow an unauthenticated, remote attacker to execute code on the affected systems. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications configured to have fewer restrictions on the system could be less impacted than those who operate with elevated privileges.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

Figure 9: A small snippet of the alerts posted by CIS. The alerts give an overview of the advisory, currently affected systems as per the CVE, and mitigation responses. The content of each alert is like I-WARN since they focus on brief mitigation tactics and links for further, in-depth dive on each response. CIS, just like I-WARN, utilizes standard visualization and content delivery as federal and state agencies in the US.

This indicates that the content of each alert is very similar to I-WARN, based on the incident described, as we mimic the contents provided by federal/state cybersecurity organizations. Given that CIS utilizes the same resources to populate its alerts, the content is very similar to I-WARN. Though some of the content comes from more technical OSINT, we believe that it is appropriate to compare our system due to the style of delivery. It should also be noted that although it curates the information from various sources, CIS does not create its own mitigation responses, but rather forwards the original ones posted in the CVE or TLP White.

INFORMAL SYSTEMS

When comparing I-WARN to all possible systems, it is imperative that informal systems are also considered since many channels of OSINT are derived through such platforms.

Twitter: One of the most common information sharing platform which is not governed by a single entity or organization is Twitter. The social media is very versatile that can be used as part of OSINT, as well as a knowledge sharing platform. Various cybersecurity organizations send out tweets, for example Figure 8, that are not as organized as the formal systems discussed previously, but send out information about incidents in a timely manner.

When looking at tweets from the perspective of information sharing, tweets do not contain all the content that systems such as I-WARN would. Given the almost-instantaneous information sharing of tweets, organizations are not able to share all the IOCs and possible mitigation response in time as a tradeoff.

The Hacker News on Twitter: We observed The Hacker News as part of our informal knowledge sharing [47]. The Hacker News is very active on Twitter in releasing information about cybersecurity events. For ease of access, they tag their tweets with #cybersecurity that makes the tweets grab attention for interested readers. Further, The Hacker News covers a diverse range of incidents which do not necessarily overlap with any government alerts as seen on ASCS or CISA. Because The Hacker News have their own cybersecurity researchers and journalists, they are able to invest in resources to collect information for domestic and international incidents.

However, as discussed before (and seen in Figure 8), the tweets are shared in high frequency which does not give enough time for The Hacker News or any other independent

source to collect and analyze all the possible IOCs and give any mitigation recommendation. Although it is faster in delivery of intelligence, I-WARN contains more details about the stories that are posted in the system as compared to The Hacker News tweets[3].

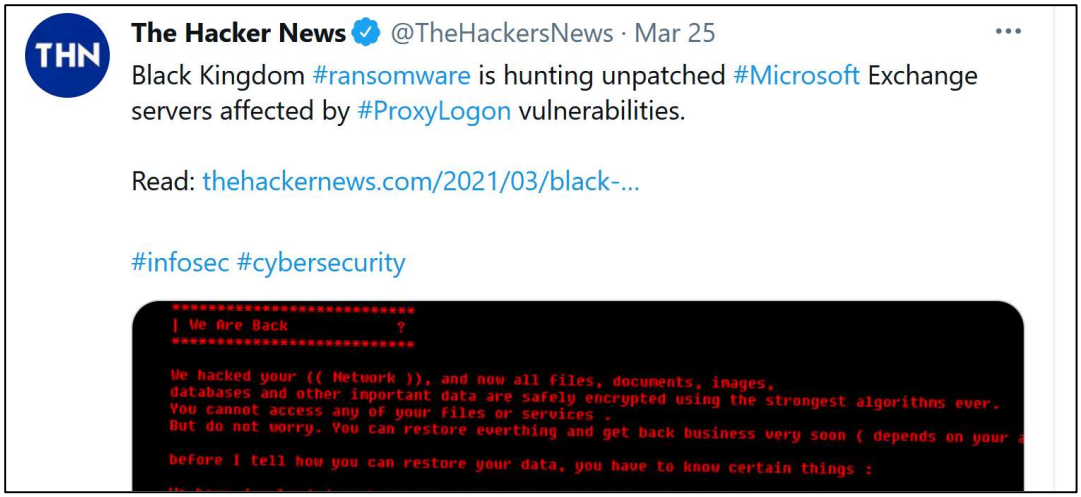


Figure 10: A tweet snapshotted from The Hacker News showing us information sharing through Twitter – part of OSINT. Although the information is informal and lacks all the contents of detection and mitigation tactics, as seen in CISA and I-WARN, the time of delivery is significantly lower due to its informal style of delivery.

Independent sources on Twitter: Other informal sources posting information related to cybersecurity incidents and stories are independent sources and individuals that do not systematically hunt and post incidents. For instance, media outlets, such as Wall Street Journal (@WSJCyber), would inform the public about cyber security incidents.

[3] Does not include retweets by The Hacker News from other organizations.

However, their cyber news does not always cover incidents, but also politics that involve cyber news. This unreliability makes such sources a weak comparison against I-WARN due to its dedicated approach to share OSINT and mitigation recommendations. Sources such as journalists and news media does not tweet about stories related to security incidents as often as the updated databases used by systems like ITAP. This results in the media tweet about cyber security and related policies, but does not overlap content or delivery time with I-WARN.

Cyware: Other platforms that we compare I-WARN to are independent websites such as Cyware [48] that releases news about cybersecurity incidents and related policies. Cyware as a system is able to separate out news relating to incidents and policies, which makes it easier for the reader to access the content of their choosing.

This compares well with I-WARN as it gives users the ability to choose the information they require from each sector. Further, since Cyware itself does not post the alerts, but rather links and highlights the alerts from different websites. It is a fast delivery system that can be monitored at a high frequency for any updates. A snippet of its platform can be seen in Figure 9. Since it links the readers to websites like The Hacker News, we see the same issue as described above: in the tradeoff for timely alerts, there is not enough information to analyze the IOCs for any detection or mitigation responses. Although websites like Cyware can deliver alerts and notifications faster than I-WARN, they do not have the same content to recommend any proactive or reactive actions for their readers.

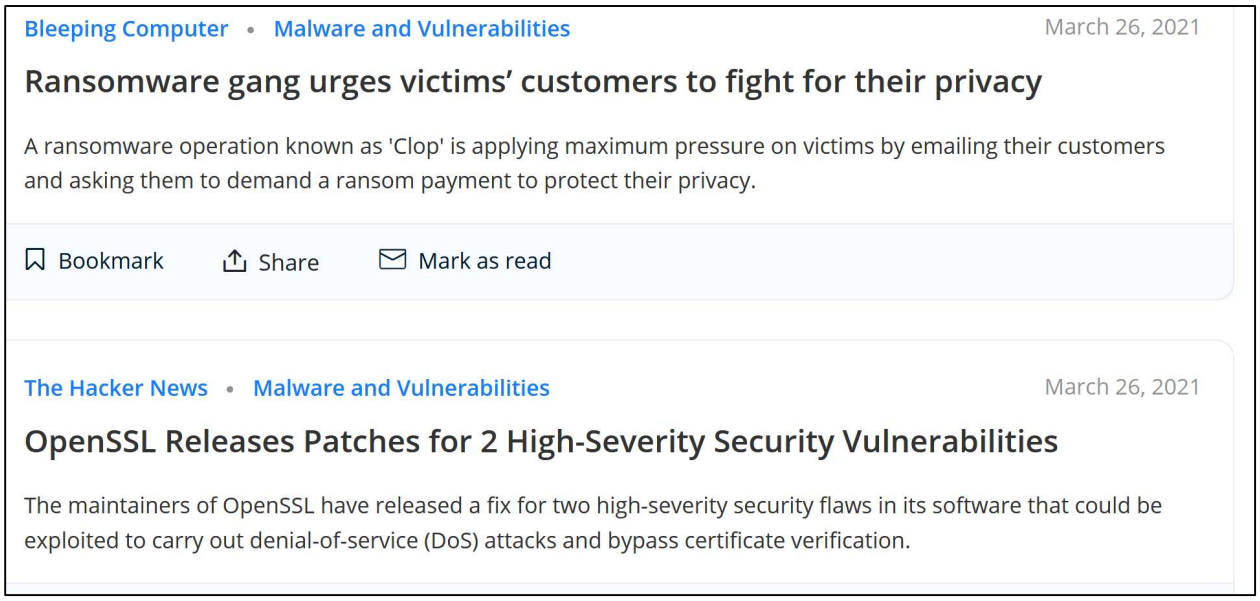


Figure 11: Snippet of the website Cyware and its alerts and notifications for cyber incidents that are not related to policies. It should be noted that Cyware does not create these articles and only curates them. This results in Cyware linking other websites like The Hacker News that may not have all the information for a proactive or reactive response.

Overall, I-WARN as a system can deliver the same content as the widely trusted sources – be it governmental or independent. The sources are pulled from the ITAP dataset that reads in stories from multiple sources, diversifying the pool as compared to governmental sources only. Further, the dedicated functionality of I-WARN enables it to share information based on technical details of the story and be available as a platform which can be accessed by devices connecting to other informal and formal systems. I-WARN is culmination of the formal and informal sources features: it is a system that aims to deliver content as dense as formal systems, but in a proactive manner like informal systems.

Chapter 5: *Future Work*

As we conclude our work, we highlight some plans for any future work.

KEEPING THE SYSTEM OPEN-SOURCE AND LIVE

One of the near-future goals for I-WARN is to be live and accessible by public-facing internet. With the Python webhook developed, we are currently exploring options of Amazon Web Services through Elastic Beanstalk [51] due to its ease of pushing Python Flask webhooks. Through Beanstalk, we will be able to store the source code to an S3 bucket and have an open connection to the webpage through port 80. Although security and having HTTPS traffic is vital and in consideration, our priority is to have a live page first. We will continue to explore other options in the realm of AWS to bring the application up and usable for the public.

All in all, though I-WARN is a system that aids in turning OSINT into actionable intelligence, the system is far from perfect. With our step in the right direction, we hope to continue our work for the betterment of organizational defenses through gather more intelligence from around the globe, streamlining our pipelines from ITAP dataset to webpage using Machine Learning, using MITRE to its full ability, and bringing the system live for the world to view and use. These expectations would ensure that I-WARN is a relevant system when threat intelligence is discussed as a topic.

COLLECTING INFORMATION FROM MORE SOURCES

One of the planned, near future work for I-WARN is expanding the resource pool of OSINT gathered.

Currently, I-WARN relies on information gather from various outlets for ITAP. Although it provides a versatile set of data for mitigation efforts to be displayed, we are

hoping to expand to add more sources and increase the information flow for the ITAP dataset to work with. Higher globalization and interconnectivity results in being connected to one part of the world, while sitting in at the other side. Although this globalization makes the world a smaller place for people to connect, unfortunately, it brings global threats to organizations or individuals' Homefront as well.

We plan on incorporating news sources from all over the globe, such as 9news from Australia [49], Economic Times from India [50], etc. It would ensure preventive measures are recommended based on threats which are not just currently present in the US, but also all around the world. With a broader scale of events being digested by I-WARN, readers for any sector will be able to better picture the shape of their market sector on a global scale and prepare their cybersecurity measures accordingly. Not only will they be able to focus on threats already occurring in the US, but also be able to proactively prepare themselves, if their organization has any open communication or any relation with countries of interest based on the ITAP dataset. With the location in mind, I-WARN aims to distinguish source of the story in addition to the distinguished sectors, giving the reader a better idea of where the incidents are occurring and if investing in mitigation recommendations is necessary for them.

USING MACHINE LEARNING

The current ITAP dataset has been manually parsed to extract all the information from each story. Although the process is very thorough, it leaves room for errors due to subjectivity and is in general very crude and cumbersome. Similarly, I-WARN logic mapping is manually integrated, leaving room for the same issues. As part of future work, we plan on utilizing the upcoming machine learning models to train on the current ITAP

dataset and logic such that keywords and inputs can be automatically extracted. With the addition of new sources, manually parsing through all stories will be rendered ineffective soon and use of ML is going to be imperative should ITAP and I-WARN keep digesting of new information on a very high frequency. The University of Texas's Center for Identity is currently working on using ML to automate all capturing of needed information for the ITAP dataset. With the models, I-WARN will be able to integrate new stories and update its dashboard on a higher frequency, as the new information is fed in. Further, we aim to work on ML models for I-WARN to be able to incorporate newer keywords and inputs as the stories add more detail. This will especially be useful when synonymous for various keywords – such as "medical centre" instead of "hospitals" – can be seen in use for news sources in other parts of the world. It would also aid in incorporating different inputs which can be used for different threat techniques and tactics as new vectors for attack surface.

Using ML, we can streamline the process of parsing through incoming sources, collecting inputs and steps taken by the bad actor, as well as map them to specified threat tactic and techniques. It will aid in fully narrowing down the mitigation recommendations, leveraging the full power of OSINT and benefitting the communities.

INCORPORATING ALL MITRE TECHNIQUES

One of the limitations discussed in Chapter 3 was the elimination of several techniques that could not be mapped to any stories in ITAP due to the lack of technical context in the current media outlets. With the increasing interdependence of information sharing and growing interest of cyber and information security in public and private organizations, we hope that OSINT retrieved from media outlets will start to provide more context on the technical details of various cyber incidents. Through the technical insights,

we would be able to incorporate the keywords retrieved into I-WARN's scoring system and provide narrowed mitigation efforts for the different techniques being utilized by the bad actors.

Due to the required efforts of organizations which I-WARN relies on, we keep this as an attainable goal for distant future. The needed evolvement of OSINT will require fundamental changes on media's information sharing procedures, foreshadowing a long wait for the technical details to be shared in story. Regardless of the wait, it is an imperative work which needs to be incorporated whenever possible. As leaders in I-WARN's covered sectors, all information collected to provide mitigation tactics can result in preventing their organizations suffer immeasurable or irreversible damage. The more threat techniques we cover, the better it is for defending organizations.

Chapter 6: *Conclusion*

This research project delivered I-WARN, an actionable identity threat intelligence and analysis tool with recommendations to mitigate and thwart threats, leveraging the integration of open sources (e.g., news media), the UT Center for Identity Threat Assessment and Prediction (ITAP) project data, and the MITRE ATT&CK framework. I-WARN ensures leaders are better prepared for cyber threats observed in the community.

Through different regulations around the globe and in the United States, information sharing is becoming a vital tool in keeping up with wide ranging, complex threat landscape. Especially within the US, agencies such as Cybersecurity and Infrastructure Security Agency (CISA) aim to alert the public and organizations of any threats and incidents that aim at critical infrastructures or the nation and its security. Though CISA aims to provide actionable intelligence, the agency does not invest in preventing lesser-known, domestic threats that affect business – small or large – and individuals alike.

I-WARN aims to fill that gap to analyze and report on emerging threats from a wide range of market sectors and incorporate the MITRE ATT&CK framework mitigation tactics to create actionable intelligence and proactively thwart threats instead of reacting after an attack. Through I-WARN, organizations of any scale can proactively get information about cyber incidents, their market sector's trends, and possible mitigation efforts. I-WARN fills the intelligence void of delivering actionable intelligence in a timely manner with formats and content that is easily understood by the organizations and leadership.

Using ITAP dataset, I-WARN can utilize openly available information, such as inputs and steps used by attackers, to map them with the current ATT&CK framework that

enables getting actionable data for readers and leaders of various market sectors. It is incredible to see how trivial information received from various media outlets, like blogposts and articles, can be turned in a power tool to better the defenses of organizations.

Through the system, I-WARN can take stories of various incidents, like as with phishing incidents, in which the attackers intrude a target system, pair them to the ATT&CK framework to understand the various threat tactics used, and create a list of mitigation tactics to recommend defenders thwart the attacks at various lateral movement. I-WARN aids in collecting such intelligence from stories that enable leaders in such market sectors to understand the technicalities of an attack from an informal source and ensure that their defenses are on par to tackle these threats should they be faced with a similar incident.

Threat Intelligence is one of the strongest tools a cyber-defending team has in its arsenal. In the battle between attackers and defenders, attackers bring the advantage of weaponizing new vulnerabilities that defenders must reactively respond to. With threat intelligence aiding the defenders to proactively know about a threat, we hope that I-WARN delivers a significant advantage to the defenders by increasing the actionable intelligence available for organizations and their leadership.

Bibliography

1. "Cyber Threat Intelligence 101." FireEye, www.fireeye.com/mandiant/threat-intelligence/what-is-cyber-threat-intelligence.html#What-is-Cyber-Threat-Intelligence
2. Bromiley, Matt. *Threat Intelligence: What It Is, and How to Use It Effectively*. NSFOCUS, Sept. 2016, nsfocusglobal.com/wp-content/uploads/2017/01/SANS_Whitepaper_Threat_Intelligence__What_It_Is__and_How_to_Use_It_Effectively.pdf.
3. Fasulo, Phoebe. "What Is Cyber Threat Intelligence? A Complete Guide." *Security Ratings & Cybersecurity Risk Management*, Security Scorecard, Mar. 2020, securityscorecard.com/blog/what-is-cyber-threat-intelligence-3-types-and-examples.
4. Zhou, Shengping, et al. "Automatic Identification of Indicators of Compromise Using Neural-Based Sequence Labelling." ArXiv:1810.10156 [Cs], Oct. 2018. arXiv.org, http://arxiv.org/abs/1810.10156.
5. Luiijf, Eric, and Marieke Klaver. "On the Sharing of Cyber Security Information." *Critical Infrastructure Protection IX*, edited by Mason Rice and Sujeet Shenoi, Springer International Publishing, 2015, pp. 29–46. *Springer Link*, doi:10.1007/978-3-319-26567-4_3.
6. Goldsmith, Jack, and Stuart Russell. *Strengths Become Vulnerabilities*. Jun. 2018, www.hoover.org/research/strengths-become-vulnerabilities.
7. Karp, Brad. "Federal Guidance on the Cybersecurity Information Sharing Act of 2015." *The Harvard Law School Forum on Corporate Governance*, Harvard, 3 Mar. 2016, corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.
8. "Corporate Overview." *The MITRE Corporation*, 28 Oct. 2020, www.mitre.org/about/corporate-overview.
9. Pennington, Adam, et al. "Getting Started with ATT&CK." *Getting Started*,MITRE,Oct.2019, www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf.
10. *MITRE ATT&CK*®, MITRE, May 2015, attack.mitre.org/.
11. Steele, Robert David. "Open Source Intelligence." *Handbook of Intelligence Studies*, by Loch K. Johnson, Routledge, 2007, pp. 129–148, books.google.com/books?id=fXeTAgAAQBAJ&dq=open+source+intelligence&lr=.
12. Williams, Heather J., and Ilana Blum. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND Corporation, 2018, doi.org/10.7249/RR1964.

13. Zaeem, Razieh Nokhbeh, et al. “Modeling and Analysis of Identity Threat Behaviors through Text Mining of Identity Theft Stories.” *Computers & Security*, Elsevier Advanced Technology, 9 Nov. 2016, www.sciencedirect.com/science/article/pii/S0167404816301559.
14. Dandurand, Luc, and Oscar Serrano. “Towards Improved Cyber Security Information Sharing.” *IEEE Xplore*, June 2013, ieeexplore.ieee.org/document/6568369.
15. White House. “Presidential Policy Directive -- United States Cyber Incident Coordination.” *National Archives and Records Administration*, National Archives and Records Administration, Dec. 2016, obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
16. ACSC. “Australian Cyber Security Centre 2016 Cyber Security Survey.” *Australian Cyber Security Centre*, Australian Signals Directorate, Mar. 2019, www.cyber.gov.au/sites/default/files/2019-03/ACSC_Cyber_Security_Survey_2016.pdf.
17. Costigan, Sean, et al. “DEEP: Cybersecurity - A Generic Reference Curriculum.” *NATO*, North Atlantic Treaty Organization, 3 Aug. 2018, www.nato.int/cps/en/natohq/topics_157591.htm.
18. Hughes, Rex B. “NATO and Cyber Defence: Mission Accomplished?” *Atlantisch Perspectief*, vol. 33, no. 1, 2009, pp. 4–8. *JSTOR*, www.jstor.org/stable/45280023. Accessed 11 Mar. 2021.
19. FBI. “Internet Crime Complaint Center (IC3) : Home Page.” *FBI and IC3 Seals*, Federal Bureau of Investigation, Apr. 2000, www.ic3.gov/.
20. Decker, Eileen. "Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score." Journal of National Security Law and Policy, vol. 10, no. 3,2020, p. 583-604. Hein Online.
21. FBI. “2019 Internet Crime Report.” *IC3*, FBI, 2020, www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf.
22. FBI. “IGuardian.” *FBI*, FBI, 31 May 2016, www.fbi.gov/resources/law-enforcement/iguardian.
23. CISA. “Critical Infrastructure Sectors.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/critical-infrastructure-sectors.
24. Secret Service. *United States Secret Service*, United States Secret Service, 1995, www.secretservice.gov/investigation/cyber.
25. CISA. “Alerts.” *Cybersecurity and Infrastructure Security Agency CISA*, 2021, us-cert.cisa.gov/ncas/alerts.
26. CISA. “Alert (AA20-258A).” *Cybersecurity and Infrastructure Security Agency CISA*, Sept. 2020, us-cert.cisa.gov/ncas/alerts/aa20-258a.
27. Center for Identity. “ITAP Report 2018.” *UT Center for Identity*, The University of Texas at Austin, May 2018, identity.utexas.edu/sites/default/files/2020-09/ITAP_Report_2018.pdf.

28. Verizon. “2020 Data Breach Investigations Report.” *Data Breach Investigations Report*, Verizon, 2020, enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
29. “VERIS The Vocabulary for Event Recording and Incident Sharing.” *The VERIS Framework*, 2013, veriscommunity.net/.
30. Crowdstrike. “Falcon X Recon: Situational Awareness: Threat Intelligence: CrowdStrike.” *Crowdstrike.com*, 18 Feb. 2021, www.crowdstrike.com/products/threat-intelligence/falcon-x-recon/.
31. IBM. *IBM X-Force Exchange*, IBM, 2015, exchange.xforce.ibmcloud.com/.
32. Chronicle Security. *VirusTotal*, 2021, www.virustotal.com/gui/home.
33. Gu, Xian, et al. “Selling the Premium in Freemium.” *Journal of Marketing*, vol. 82, no. 6, SAGE Publications, 2018, pp. 10–27, doi:10.1177/0022242918807170
34. Protalinski, Emil. “Alphabet's Chronicle Launches VirusTotal Enterprise with Private Graph and 100-Times Faster Malware Search.” *VentureBeat*, VentureBeat, 28 Sept. 2018, venturebeat.com/2018/09/27/alphabets-chronicle-launches-virustotal-enterprise-with-private-graph-and-100-times-faster-malware-search/.
35. CISA. “Cybersecurity Framework.” *Cybersecurity and Infrastructure Security Agency CISA*, Feb. 2013, us-cert.cisa.gov/resources/cybersecurity-framework.
36. Crowdstrike. “2021 Global Threat Report.” *Global Threat Reports*, Crowdstrike, 2021, www.crowdstrike.com/resources/reports/global-threat-report/.
37. H. M. Farooq and N. M. Otaibi, "Optimal Machine Learning Algorithms for Cyber Threat Detection," *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, Cambridge, UK, 2018, pp. 32-37, doi: 10.1109/UKSim.2018.00018.
38. Zilberman, Polina, et al. “SoK: A Survey of Open-Source Threat Emulators.” *ArXiv:2003.01518 [Cs]*, Oct. 2020. *arXiv.org*, http://arxiv.org/abs/2003.01518
39. Hartong, Olaf, and Nihlander. “Red Team Automation (RTA).” *Github*, Endgameinc, 2018, github.com/endgameinc/RTA.
40. Rantala, Ramona R. “Cybercrime against Businesses, 2005.” *Cybercrime*, Bureau of Justice Statistics, 2008, www.bjs.gov/content/pub/pdf/cb05.pdf.
41. Harrell, Erika. “Victims of Identity Theft, 2016.” *Identity Theft*, Bureau of Justice Statistics, Jan. 2019, www.bjs.gov/content/pub/pdf/vit16.pdf.
42. Pallets Projects. *Flask*. 2018, github.com/pallets/flask.

43. Google Charts. “Visualization: Pie Chart | Charts | Google Developers.” *Google*,Google,2007, developers.google.com/chart/interactive/docs/gallery/piechart.

44. ACSC. “View All Alerts.” *Cyber.gov.au*, 2014,

www.cyber.gov.au/acsc/view-all-content/alerts.

45. Center for Internet Security. “CIS®.” *CIS*, 2021, www.cisecurity.org.
46. CISA. “Traffic Light Protocol (TLP) Definitions and Usage.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/tlp.
47. “Cybersecurity News and Analysis.” The Hacker News, 2007, thehackernews.com/.
48. Cyware Labs. “Cyber Security News Today: Articles on Cyber Security, Malware Attack Updates: Cyware.” Cyware Labs, 2016, cyware.com/cyber-security-news-articles.
49. 9News. *Cyber Security News Headlines*. www.9news.com.au/cyber-security.
50. Economic Times. “Cybersecurity News - Latest Cybersecurity News, Information & Updates - IT News -ET CIO.” *ETCIO.com*, Economic Times, cio.economictimes.indiatimes.com/tag/cybersecurity.
51. Vliet, Jurg van. “Elastic Beanstalk.” *Amazon*, O'Reilly, 2011, docs.aws.amazon.com/elastic-beanstalk/index.html.
52. Chang, Kai Chih, et al. “Internet of Things: Securing the Identity by Analyzing Ecosystem Models of Devices and Organizations.” *AAAI Publications, 2018 AAAI Spring Symposium Series*, AAAI, Mar. 2018, aaai.org/ocs/index.php/SSS/SSS18/paper/view/17491.
53. Zaeem, Razieh Nokhbeh, et al. “Predicting and Explaining Identity Risk, Exposure and Cost Using the Ecosystem of Identity Attributes.” *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, IEEE, Jan. 2017, ieeexplore.ieee.org/document/7815701.
54. Barber, Suzanne. *Identity Threat Assessment and Prediction (ITAP)*, Keesing Platform, 16 Oct. 2019, platform.keesingtechnologies.com/identity-threat-assessment-and-prediction-itap/.
55. Liau, David, et al. “Evaluation Framework for Future Privacy Protection Systems: A Dynamic Identity Ecosystem Approach.” *2019 17th International Conference on Privacy, Security and Trust (PST)*, IEEE, Jan. 2016, ieeexplore.ieee.org/document/8949059.
56. Rana, Rima, et al. “US-Centric vs. International Personally Identifiable Information: A Comparison Using the UT CID Identity Ecosystem.” *2018 International Carnahan Conference on Security Technology (ICCST)*, IEEE, Dec. 2018, ieeexplore.ieee.org/document/8585479.

57. Chen, Chia-Ju, et al. “Statistical Analysis of Identity Risk of Exposure and Cost Using the Ecosystem of Identity Attributes.” *2019 European Intelligence and Security Informatics Conference (EISIC)*, IEEE, June 2020, ieeexplore.ieee.org/document/9108859.
58. Liau, David, et al. “An Evaluation Framework for Future Privacy Protection Systems: A Dynamic Identity Ecosystem Approach.” *ICAART20-RP-41: Short Paper*, INSTICC, 2020, www.insticc.org/node/TechnicalProgram/icaart/2020/presentationDetails/89135.
59. Kuperberg, Michael. “Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective.” *IEEE Transactions on Engineering Management*, IEEE, Aug. 2019, ieeexplore.ieee.org/document/8792372.
60. Rana, Rima, et al. “An Assessment of Blockchain Identity Solutions: Minimizing Risk and Liability of Authentication.” *2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, IEEE, Nov. 2019, ieeexplore.ieee.org/abstract/document/8909638.
61. Chang, Kai Chih, et al. “Is Your Phone You? How Privacy Policies of Mobile Apps Allow the Use of Your Personally Identifiable Information.” *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, IEEE, Jan. 2021, ieeexplore.ieee.org/document/9325370.
62. David Liau, et al. “A Survival Game Analysis to Personal Identity Protection Strategies.” *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, IEEE, Jan. 2021, ieeexplore.ieee.org/abstract/document/9325424/references#references.
63. Chang, Kai Chih, et al. “Enhancing and Evaluating Identity Privacy and Authentication Strength by Utilizing the Identity Ecosystem.” *WPES'18: Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, ACM, Jan. 2018, dl.acm.org/doi/abs/10.1145/3267323.3268964.
64. Chang, Kai Chih, et al. “A Framework for Estimating Privacy Risk Scores of Mobile Apps.” *International Conference on Information Security, ISC 2020: Information Security Pp 217-233*, SpringerLink, Nov. 2020, link.springer.com/chapter/10.1007/978-3-030-62974-8_13.
65. Zaeem, Razieh Nokhbeh, et al. “Risk Kit: Highlighting Vulnerable Identity Assets for Specific Age Groups.” *2016 European Intelligence and Security Informatics Conference (EISIC)*, IEEE, Mar. 2017, ieeexplore.ieee.org/document/7870187.
66. TalkersCode. “Expand Table Rows Using JQuery, HTML And CSS (May 2020).” *A Web Development And Internet Marketing Blog*, TalkersCode,

Feb. 2020, talkerscode.com/webtricks/expand-table-rows-using-jquery-html-and-css.php.
67. Robert. *Barking Up the Wrong Tree(?): HTML/CSS Iframe for Dynamic Dropdown Menus*, Velo, 8 May 2020, www.wix.com/velo/forum/coding-with-velo/barking-up-the-wrong-tree-html-css-iframe-for-dynamic-dropdown-menus.